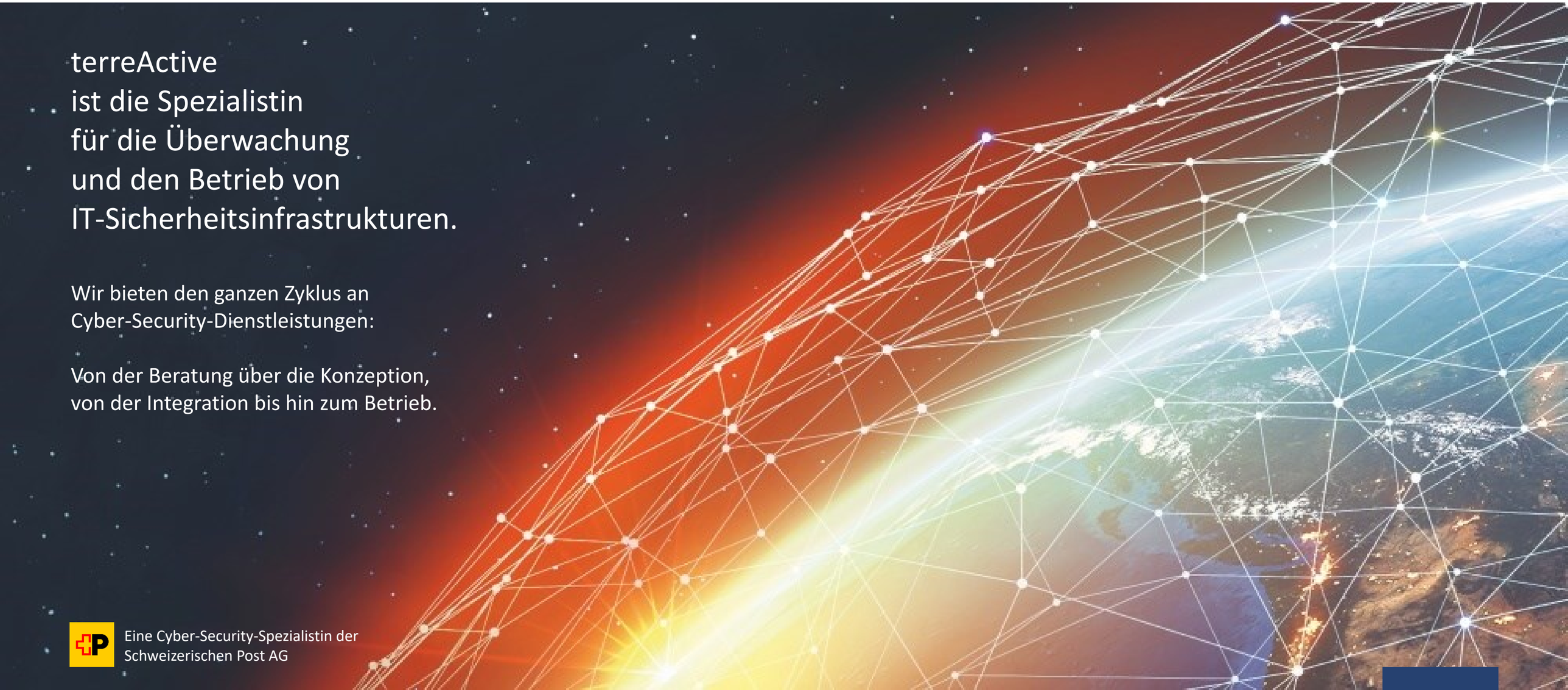
terreActive AG

Über uns



terreActive
ist die Spezialistin
für die Überwachung
und den Betrieb von
IT-Sicherheitsinfrastrukturen.

Wir bieten den ganzen Zyklus an
Cyber-Security-Dienstleistungen:

Von der Beratung über die Konzeption,
von der Integration bis hin zum Betrieb.

Eine Cyber-Security-Spezialistin der
Schweizerischen Post AG

Das Profil

Über uns

Beständigkeit:
Gründung 1996

> 25 Jahre Kompetenz in der Cyber Security

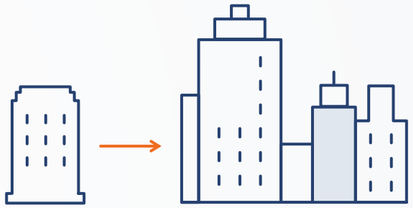
Schweizer Firma

Mitarbeitende:
rund 60 von 90 sind ausgebildete Ingenieure

Gründerduo steht für Kontinuität

Kernkompetenz:
Beratung und Betrieb

Das CDC macht 75 % unseres Geschäfts aus



Kunden:
Firmengrössen vom KMU bis zum Grosskonzern

Berücksichtigung von branchenspezifischen Besonderheiten

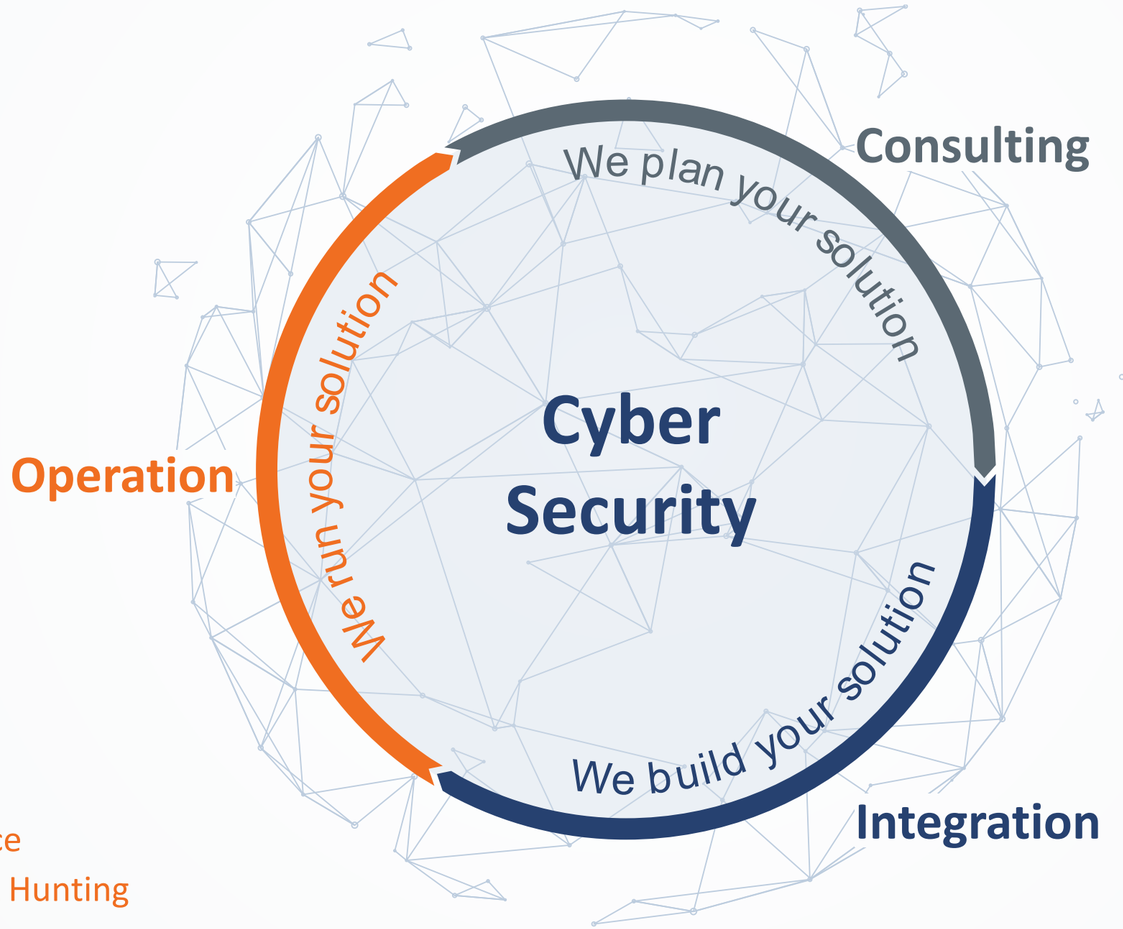
© terreActive AG

Das Angebot

Unsere Services für Ihre Sicherheit

- Concepts
- Assessments
- Architectures
- Cyber Deception
- Risk & Compliance

- Audits
- Penetration Tests
- Vulnerability Scan
- Social Engineering
- Phishing Simulation
- Awareness Trainings



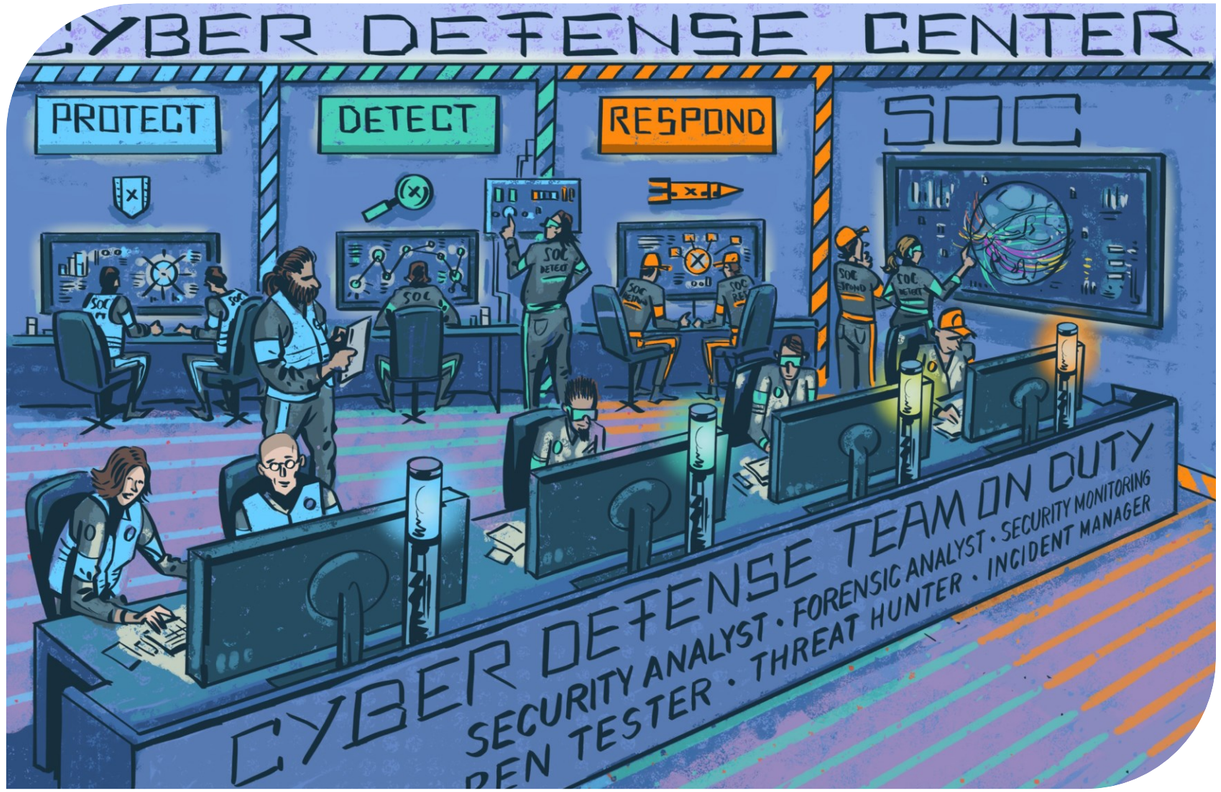
- SOC Services
- Forensic Analysis
- Incident Response
- SOAR-as-a-Service
- Operations Control
- Security Monitoring
- Vulnerability Management
- Managed Security Services
- System Monitoring & Maintenance
- Threat Detection & Intelligence & Hunting

- WAF
- SIEM
- Firewall
- Network Security
- Log Management
- Application Security
- Web & E-Mail Security
- Cyber Defense Platform
- Privileged Access Control

© terreActive AG

Ein SOC…

Unser Cyber Defense Center



OCC / IRC

Zusammenspiel und Abgrenzung

SOC Security Operations Center

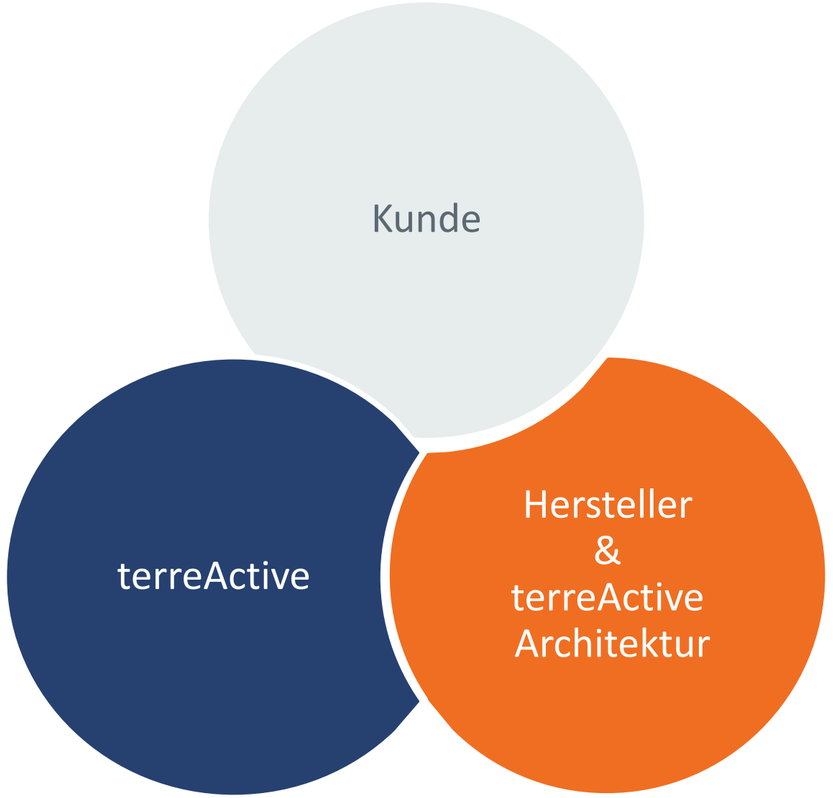
OCC Operations Control Center	**IRC** Incident Response Center
Wartung und Betrieb von IT-Infrastruktur und Software, sowie Netzwerk, Server, Applikationen	Erkennen und Bearbeiten von IT-Sicherheitsvorfällen 5x11 / 7x24
Wartung und Betrieb von IT-Sicherheitskomponenten wie Firewalls, Proxies, SIEM-Lösungen, Cloudservices	Reaktion auf Vorfälle und Folge-Support
	Forensische Analysen von Vorfällen
	Tuning und Monitoring von Lösungen

Airlock, terreActive & Kunde

Co-Creation mit allen Beteiligten – Jeder hat seine Stärken

Das «Team»

- Ergon = Hersteller
- Airlock = Produkt
- terreActive = Dienstleister (Architektur, Integration, Betrieb)



Cyber Defense Platform und weitere SOC-Services

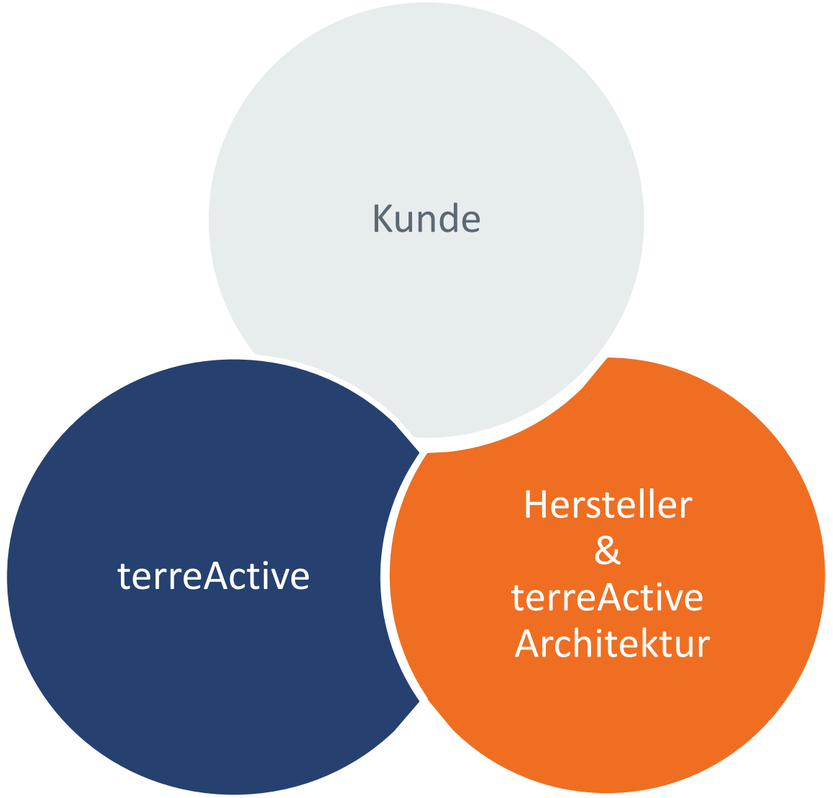
- Airlock als wertvoller Log- / Event-Lieferant
- Direkt am Perimeter mit relevanten Informationen bei einem Event und der Möglichkeit zum aktiven Eingreifen
- Verlässlich und hilfreich beim genauen Analysieren und beim Nachvollziehen von sicherheitsrelevanten Vorfällen

© terreActive AG

Kundenbeispiel: terreActive + Airlock

Ideals Setup für den Start unserer Cyber Defense Services

- Grosser Finanzdienstleister / Berater in der Schweiz
- terreActive Kunde für die sichere Authentifizierung
- Schnelle Reaktion nach Ausbruch der Pandemie für den sicheren Zugang von Remote via Multi-Faktor Authentication
- Operations-Teil (OCC) vom SOC konnte hier helfen
- Direkter Zugriff auf dem Perimeter
- Identifizieren & Reagieren
- Airlock WAF ist eine wertvolle Logquelle für den Betrieb und den Ausbau weiterer SOC-Services



© terreActive AG

Cyber Defense Fabrik

Die Fabrik für Cyber Defense bringt Synergieeffekte

SOC terreActive

SOC-Team

- Tier-1 Analyst
- Tier-2 Analyst
- Security Engineer
- Service Manager

SOC-Services

- Thread Detection
- SecMon Tuning, Enhancement
- Vulnerability Management
- SecMon Reporting Meeting

SOC Management Framework

- SOC Portal
- Monitoring / Alarming
- Ticketing / Case Mgt.
- PAM / Session Recording

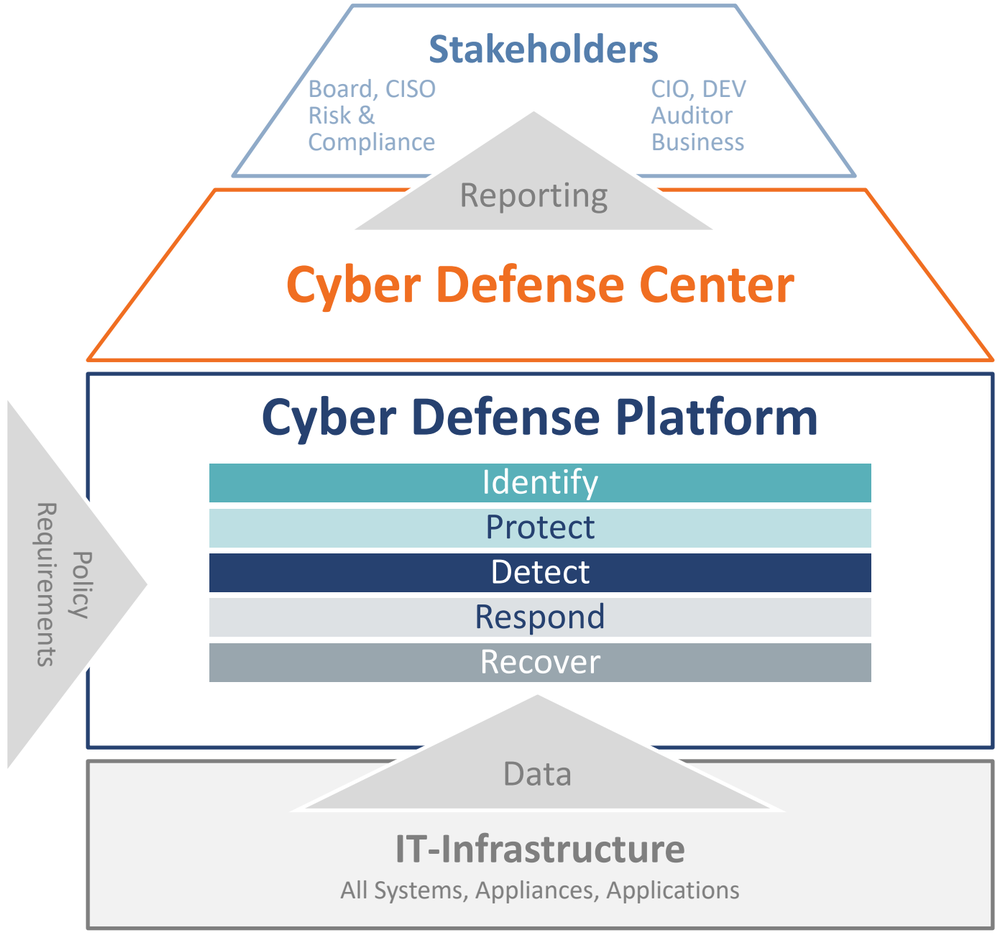
SaaS Services

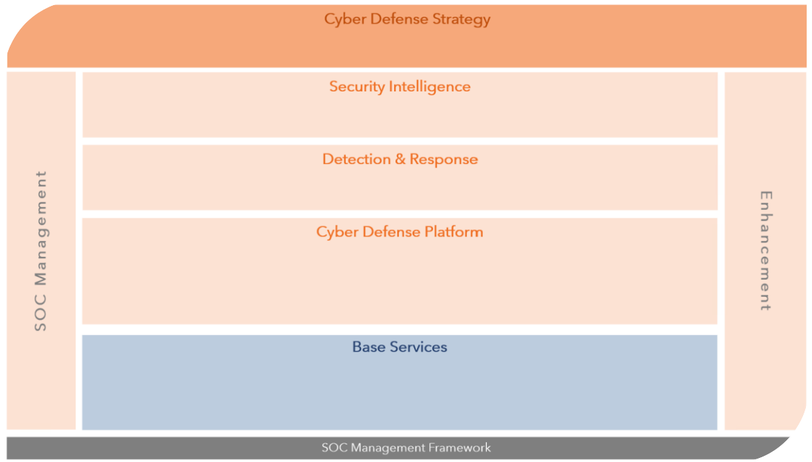
- TIFaNI Threat Intelligence Feed
- Use Case Repository & Mgmt App
- Use Case Testing
- SOC Playbooks & Runbooks
- Automation (SOAR)

Cyber Defense Plattform @Customer

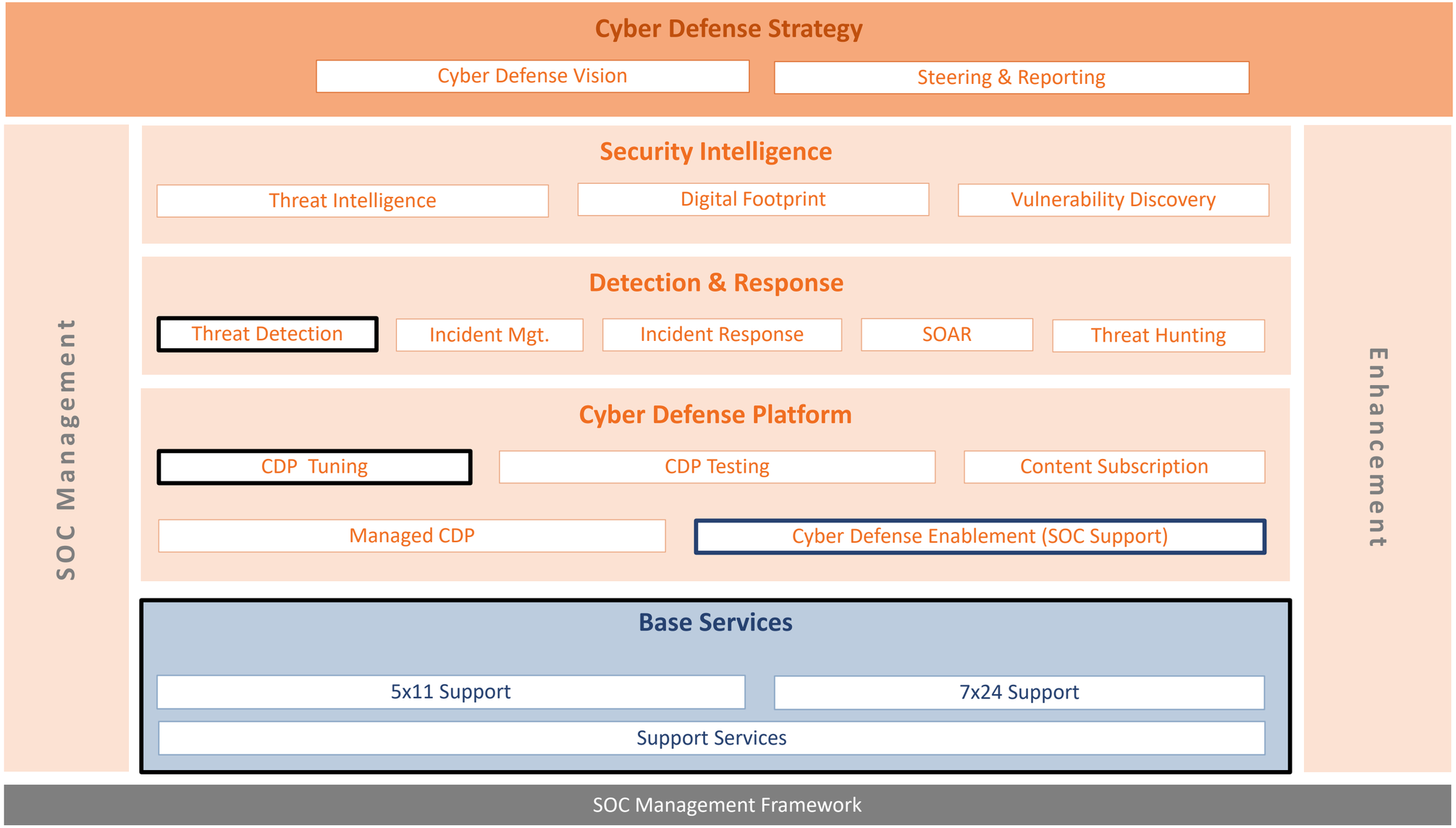
Cyber Defense

Zielbild für die SOC-Organisation





Cyber Defense Center - Servicekatalog

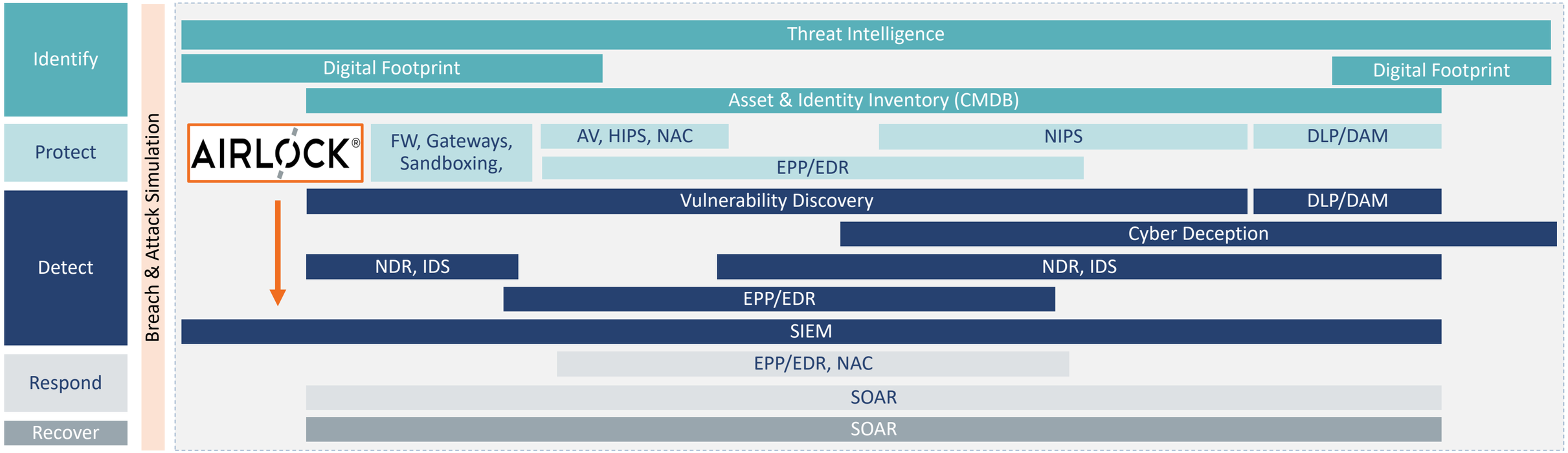


Cyber Defense Platform

Attack Phases (Cyber Kill Chain)

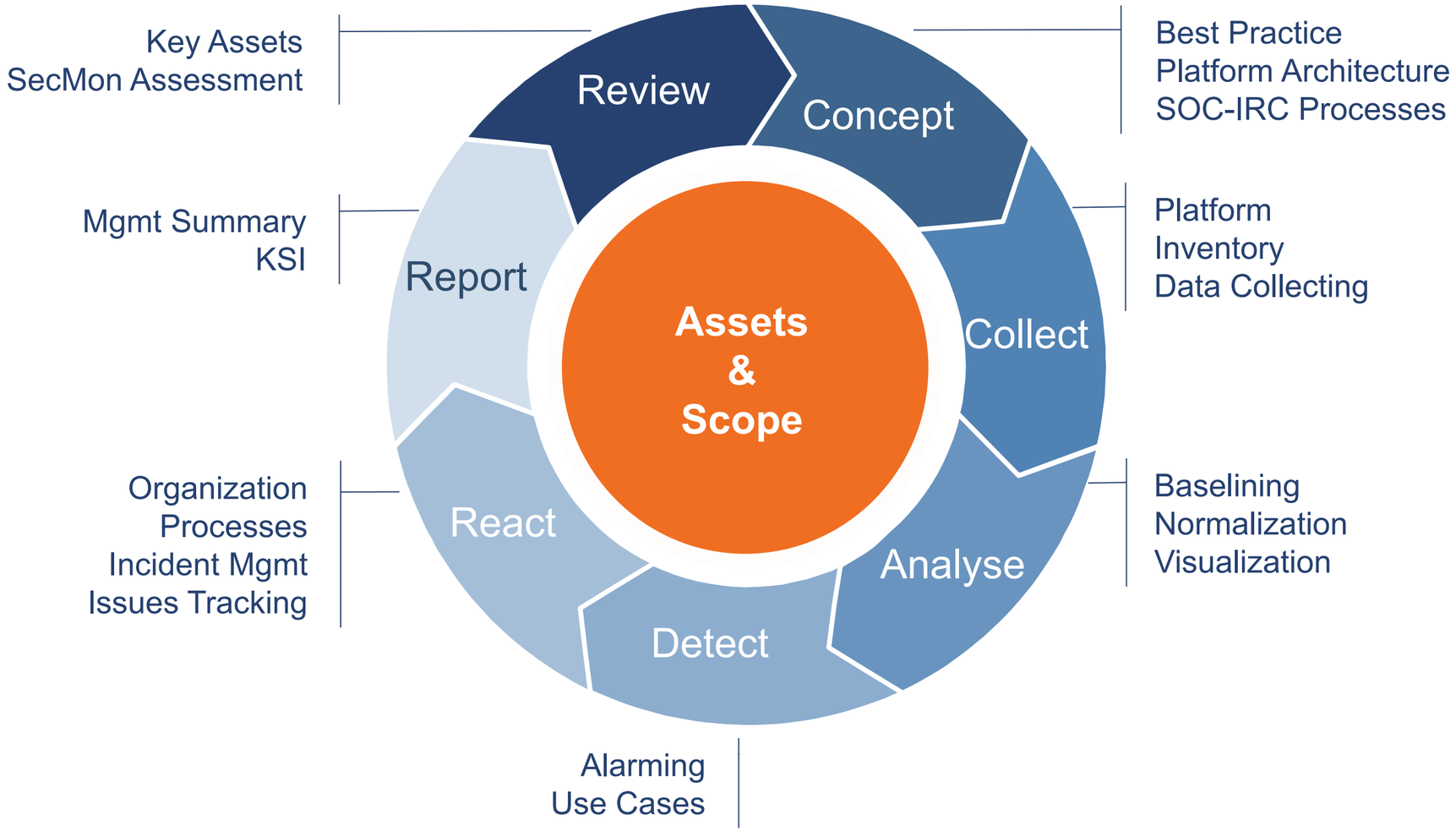
NIST

TOOLS FOR CYBER DEFENSE PLATFORM



Cyber-Defense-Projekt

Wir bauen nach dem Standardvorgehen der 7-Steps-Methodik



© terreActive AG

Cyber Defense

Der Nutzen des Threat Detection Services (typisches Beispiel)

Customer	terreActive	Customer

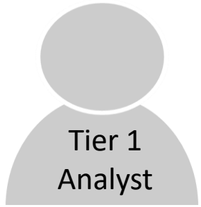
Log data
System data

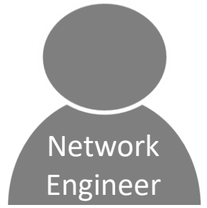
GByte/day

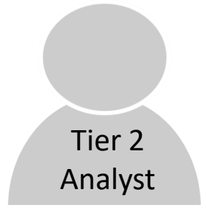
Events

MByte/day

Correlation







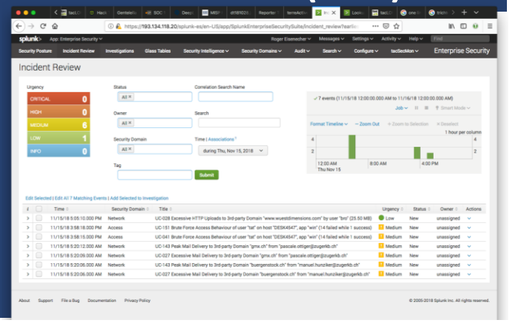
Notable Events
200/day all
5/day high, critical

Alert
1/day

Ticket

Threat Detection Service (CDP)

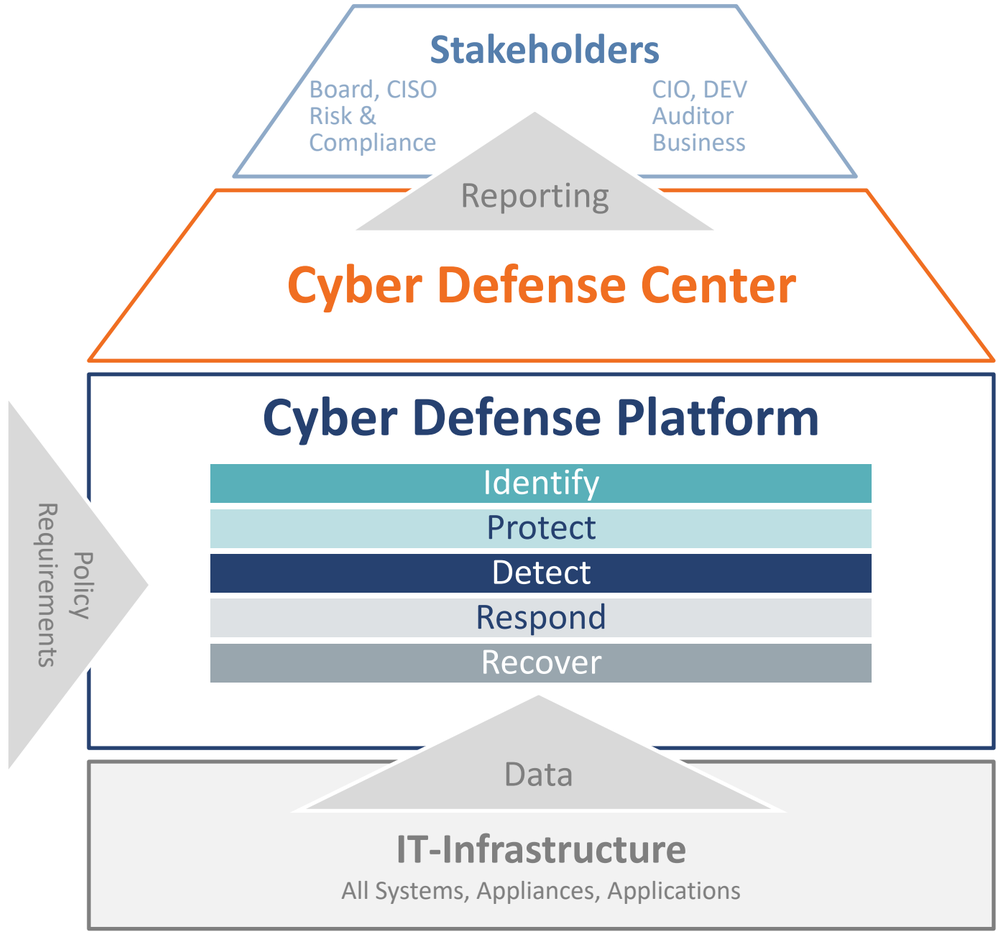
- Risk Scoring
- Direct reaction (Alert 7x24, 5x11)
- Triage (5x11)



Cyber Defense Platform (CDP) erklären

Was verstehen wir unter CDP und was bietet diese

- Konsole / Startpunkt für unsere Analysten
- Hybrid oder Cloud Setup möglich
  - Flexibles Setup basierend auf den Kundenwünschen
- Datensammlung für Analyse via SIEM
- Reaktion via SOAR (manuell oder voll automatisch)
- Weiterführend Service aufbauend wie:
  - Vulnerability Scanning
  - Digital Footprint



SOC-Services Vorteile

Ihr Nutzen mit unseren SOC-Services

Fachleute
7x24

Wochenende
Ferienzeit

Schnelle **Reaktionszeit** durch Team in der Schweiz

Threat Intelligence

Profitieren von **Erfahrungen** anderer Kunden

Kostenfaktor

%-Anteil an vers. Rollen

Modularer Servicekatalog **flexibel** an Ihre Bedürfnisse anpassbar

Kalkulierbare und kontrollierbare **Ausgaben**

Ressourcen-entlastung durch Delegation von Arbeiten

Leistungsfähige Tools

Management-, Monitoring-, Analyse- und Alarm-Software

Transparenz dank **Reporting** im Kundenportal

Damit Angreifer keine Chance haben

© terreActive AG

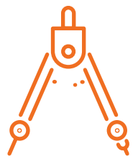
Häufige Fallstricke im Projekt

Aus der Praxis

Es ist wichtig, den Umfang des Projekts nicht zu unterschätzen. Um ein erfolgreiches Ergebnis zu erzielen, ist eine enge Zusammenarbeit unerlässlich.

Es wird zu viel über Produkte gesprochen und zu wenig über Prozesse, Aufgaben und Resultate.

Kernapplikationen & Daten: Nur wer weiss was zu schützen ist, kann auch die richtigen Massnahmen und Entscheide fällen.



Die eigenen Ressourcen und Prozesse kennen und auf die der Partner und Provider abstimmen.

Zusammenfassung

Drei Grundsätze

1. **Jeder konzentriert sich auf seine Stärken.**
   Der Kunde kennt seine IT im Detail während das SOC die nötigen Cyber-Defense-Fähigkeiten einbringt.
   Abstimmung Tooling, Prozesse und Aufgaben.
2. **Nur wer gut vorbereitet ist kennt seine Schwächen.**
   Systematisch und schrittweise die Cyber Defense etablieren und ausbauen führt zum Ziel. Nur wenn die involvierten Parteien ständig üben und daraus lernen, sind sie im Notfall bereit.
3. **Immer einen Schritt voraus sein.**
   Nur wer sich ständig weiterentwickelt, kann dem Angreifer einen Schritt voraus sein.
   Wenn der Aufwand zu hoch ist, sucht sich der Angreifer ein anderes Opfer.

Besser immer **einen Schritt voraus** zu sein!

© terreActive AG

Kontakt

Keine News mehr verpassen!
Folgen Sie uns.

Vielen Dank für Ihre Zeit.
Bei Fragen stehe ich sehr gerne zur Verfügung.

Silvan Leuenberger

Head of Service Management and Delivery

silvan.leuenberger@terreactive.ch